(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
2. Oktober 2003 (02.10.2003)

PCT

(10) Internationale Veröffentlichungsnummer
WO 03/081417 A2

(51) Internationale Patentklassifikation[7]: G06F 7/00

(21) Internationales Aktenzeichen: PCT/EP03/02436

(22) Internationales Anmeldedatum:
10. März 2003 (10.03.2003)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
102 13 269.0 25. März 2002 (25.03.2002) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **INFINEON TECHNOLOGIES AG** [DE/DE]; St.-Martin-Str. 53, 81669 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **JANSSEN, Norbert** [DE/DE]; Innere Wiener Str. 13A, 81667 München (DE).

SEIFERT, Jean-Pierre [DE/DE]; Harsdörfer Str. 1, 81669 München (DE).

(74) Anwälte: **ZINKLER, Franz** usw.; Postfach 246, 82043 Pullach bei München (DE).

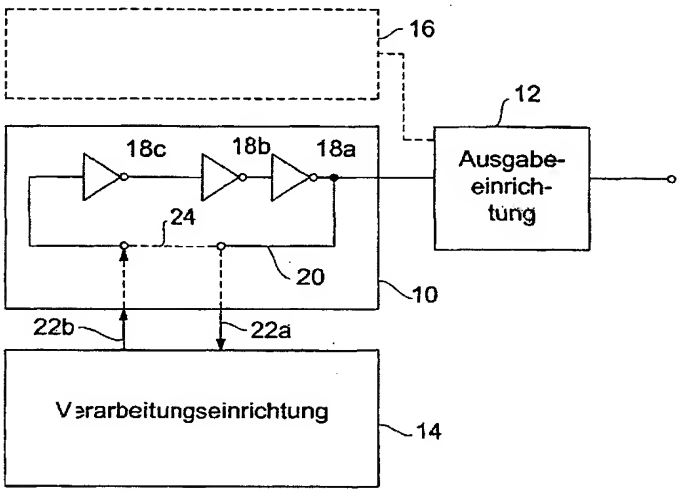
(81) Bestimmungsstaaten *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(regional)*: ARIPO-Patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL,

[Fortsetzung auf der nächsten Seite]

(54) Title: RANDOM NUMBER GENERATOR

(54) Bezeichnung: ZUFALLSZAHLENGENERATOR



12 OUTPUT DEVICE
14 PROCESSING DEVICE

(57) Abstract: The invention relates to a random number generator which comprises a closed-loop inverter chain (10) with inverters (18a, 18b, 18c) connected in series, an output device (12) for outputting a random number that depends on the status between two inverters (18a, 18c) of the closed-loop inverter chain (10), and a processing device (14) for processing a signal between two subsequent inverter chains of the inverters connected in series and for feeding the processed signal to the closed-loop inverter chain. The processing device (14) is configured in such a manner that the processed signal differs from the signal between the two subsequent inverters (18a, 18c). By specifically influencing the closed-loop inverter chain (10), the danger of the periodic scanning by means of the outputting device (12) is reduced, thereby obtaining a high-quality random number generator with reduced chip surface requirements and low power consumption.

[Fortsetzung auf der nächsten Seite]

WO 03/081417 A2

PT, RO, SE, SI, SK, TR), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— *ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(57) Zusammenfassung: Ein Zufallszahlengenerator umfasst eine rückgekoppelte Inverterkette (10) mit in Serie geschalteten Invertern (18a, 18b, 18c), eine Ausgabeeinrichtung (12) zum Ausgeben einer Zufallszahl, die von einem Zustand zwischen zwei Invertern (18a, 18c) der rückgekoppelten Inverterkette (10) abhängt, sowie eine Verarbeitungseinrichtung (14) zum Verarbeiten eines Signals zwischen zwei aufeinanderfolgenden Inverterketten der in Serie geschalteten Inverter und zum Einspeisen eines verarbeiteten Signals in die rückgekoppelte Inverterkette, wobei die Verarbeitungseinrichtung (14) so ausgebildet ist, dass sich das verarbeitete Signal von dem Signal zwischen den zwei aufeinanderfolgenden Invertern (18a, 18c) unterscheidet. Durch gezieltes Beeinflussen der rückgekoppelten Inverterkette (10) wird die Gefahr des periodischen Abtastens mittels der Ausgabeeinrichtung (12) minimiert, so dass ein hochqualitativer Zufallszahlengenerator mit kleinem Chipflächenverbrauch und kleinem Leistungsverbrauch erhalten wird.

3NSDOCID: <WO_____03081417A2_I_>

Beschreibung

Zufallszahlengenerator

Die vorliegende Erfindung bezieht sich auf Zufallszahlengeneratoren und insbesondere auf sogenannte Inverterketten-Zufallszahlengeneratoren.

Ein bekannter Inverterketten-Zufallszahlengenerator oder Inverterketten-RNG (RNG = Random Number Generator) ist in Fig. 4 dargestellt. Ein bekannter Inverterketten-Zufallszahlengenerator umfaßt eine oder mehrere unabhängig freischwingende rückgekoppelte Inverterketten primer Länge. Dies bedeutet, daß jede rückgekoppelte Inverterkette eine Anzahl von 3, 5, 7 etc. Invertern hat. Insbesondere umfaßt der bekannte Inverterketten-Zufallszahlengenerator von Fig. 4 eine erste Inverterkette 40 mit drei rückgekoppelten kaskadierten Invertern 40a, 40b, 40c und eine zweite Inverterkette 42 mit fünf rückgekoppelten kaskadierten Invertern 42a, 42b, 42c, 42d, 42e. Beide Inverterketten sind über eine Rückkopplungseinrichtung 41 bzw. 43 derart rückgekoppelt, daß der Ausgang des letzten Inverters, wie z. B. 42e, mit dem Eingang des ersten Inverters 42a verbunden ist. Die Ausgangssignale beider Inverterketten 40, 42 werden mittels eines Abtasters 44 abgetastet, wobei zum Abtasten eine externe Frequenz verwendet wird, die nicht in Beziehung zu der Frequenz steht, mit der die erste Inverterkette 40 oder die zweite Inverterkette 42 schwingt. Insbesondere muß die Abtastfrequenz niedriger als die kleinste Schwingfrequenz unter den Inverterketten sein. Anschließend wird ein Wert, der von der oberen Inverterkette 42 abgetastet worden ist, und ein Wert, der von der unteren Inverterkette 40 zum gleichen Zeitpunkt abgetastet worden ist, z. B. mittels eines XOR-Gatters 45 in ein

einziges Bit komprimiert. Somit liefert ein Abtastvorgang unter Verwendung des Abtasters 44 ein Zufallszahlenbit.

Nachteilig an dem in Fig. 4 beschriebenen bekannten Inverterketten-Zufallszahlengenerator ist, daß trotz des Frequenzunterschiedes zwischen der Schwingfrequenz der ersten und zweiten Inverterkette und des Frequenzunterschiedes zwischen diesen Schwingfrequenzen und der externen Abtastfrequenz immer oder in periodischen Abständen auf den beiden Ausgangsleitungen 46a, 46b des Abtasters 44 das gleiche Bitmuster oder Pattern ausgegeben wird. Dieses Problem ist dahingehend nachteilhaft, daß damit die Qualität des in Fig. 4 gezeigten Inverterketten-Zufallszahlengenerators drastisch reduziert wird. Insbesondere bei kryptographischen Anwendungen, bei denen die Sicherheit kryptographischer Algorithmen mit der Qualität des Zufallszahlengenerators steht und fällt, ist diese Problematik besonders nachteilhaft, da sich eine Verwendung eines Inverterketten-Zufallszahlengenerators für kryptographische Anwendungen, wie z. B. in SmartCards, eigentlich verbietet.

Eine Möglichkeit, um das beschriebene Problem zu umgehen, besteht darin, mehrere in Fig. 4 gezeigte Inverterketten-Zufallszahlengeneratoren parallel zu verwenden und dann die Ausgangssignale der XOR-Gatter der einzelnen Zufallszahlengeneratoren zu konkatinieren. Eine solche Vorgehensweise vermindert die Möglichkeit eines periodisch identischen Samplings, da dies nunmehr für alle solchen parallel betriebenen Zufallszahlengeneratoren passieren müßte. Die Wahrscheinlichkeit, daß dieser Fall für sämtliche parallel arbeitenden Zufallszahlengeneratoren auftritt, sinkt mit steigender Anzahl parallel betriebener Zufallszahlengeneratoren. Auf

diese Art und Weise ist es jedoch nicht möglich, das Problem des periodischen Samplings generell auszuschließen.

Das Verwenden mehrerer parallel betriebener Inverterketten-Zufallszahlengeneratoren ist ferner dahingehend nachteilhaft, daß mit jedem zusätzlichen Zufallszahlengenerator Chipfläche investiert werden muß, die bei vielen Anwendungen, wie z. B. für Sicherheits-ICs, begrenzt ist. Des weiteren führen mehrere Inverterketten-Zufallszahlengeneratoren zu einem erhöhten Leistungsverbrauch, der bei einer Verwendung der CMOS-Technik zwar begrenzt ist, der jedoch dann, wenn Kontaktlos-Anwendungen betrachtet werden, durchaus ins Gewicht fällt. Hier werden Zufallszahlengeneratoren allein durch eine extern empfangene HF-Energie betrieben, da Chipkarten für Kontaktlos-Anwendungen im allgemeinen selbst keine Stromversorgung haben. Jeder zusätzliche parallel betriebene Zufallszahlengenerator erhöht daher den Bedarf an Chipfläche und den Leistungsverbrauch, führt jedoch nicht zu der Erzeugung von mehr Zufallszahlen, derart, daß der Aufwand an Chipfläche und Leistung für ein Zufallsbit immer weiter ansteigt.

Die Aufgabe der vorliegenden Erfindung besteht darin, einen Zufallszahlengenerator zu schaffen, der verläßlich und effizient Zufallszahlen erzeugt.

Diese wird durch einen Zufallszahlengenerator nach Patentanspruch 1 gelöst.

Der vorliegenden Erfindung liegt die Erkenntnis zugrunde, daß das Periodizitätsproblem eines Zufallszahlengenerators mit rückgekoppelter Inverterkette dadurch behoben werden kann, daß gezielt in die Rückkopplung eingegriffen wird. Hierzu ist einer rückgekoppelten Inverterkette mit in Serie geschalteten

Invertern eine Verarbeitungseinrichtung zum Verarbeiten eines Signals zwischen zwei aufeinanderfolgenden Invertern der in Serie geschalteten Inverter vorgesehen, um das Signal zwischen den zwei aufeinanderfolgenden Invertern zu verarbeiten, so daß sich dieses Signal von einem Signal zwischen den beiden Invertern ohne Vorhandensein der Verarbeitungseinrichtung unterscheidet. Das verarbeitete Signal wird dann wieder entweder an dieselbe Stelle zwischen den beiden aufeinanderfolgenden Invertern eingekoppelt oder an einer anderen Stelle in der rückgekoppelten Inverterkette. Dadurch wird erreicht, daß die Ausgabe der Inverterkette aufgrund des Eingriffs in die Rückkopplung stark asynchron gegenüber ihrer ursprünglichen Frequenz wird, so daß, wenn eine bestimmte Abtastfrequenz verwendet wird, auch eine starke Asynchronität zur Abtastfrequenz erhalten wird.

Vorzugsweise führt die Verarbeitungseinrichtung eine nicht-lineare Verarbeitung des ausgekoppelten Signals zwischen zwei aufeinanderfolgenden Invertern durch und speist das nicht-linear verarbeitete Signal aufgrund der Einfachheit der Schaltung wieder an derselben Stelle ein, wo es ausgekoppelt worden ist.

Bei einem bevorzugten Ausführungsbeispiel der vorliegenden Erfindung umfaßt die Verarbeitungseinrichtung eine oder mehrere Kapazitäten, die zwischen der Rückkopplungsleitung und dem Massepotential geschaltet sind. Die eine oder die mehreren Kapazitäten führen zu einer hinsichtlich der Frequenz nicht-linearen Phasenverschiebung und wirken sich in einer nicht-linearen Verzögerung aus. Derselbe Effekt könnte mit seriell geschalteten Induktivitäten erreicht werden. Die Realisierung von Kapazitäten ist jedoch für integrierte Schal-

tungen aufgrund des geringeren Aufwands bei der Schaltungsintegration vorteilhaft.

Gemäß einem weiteren Ausführungsbeispiel der vorliegenden Erfindung wird es bevorzugt, in der Verarbeitungseinrichtung eine kryptographisch starke Komprimierungsfunktion zu verwenden, wie z. B. eine Hash-Funktion, eine Einweg-Funktion oder etwas ähnliches, die eine besonders starke Nichtlinearität aufweist. Alternativ kann die Verarbeitungseinrichtung auch derart ausgebildet sein, daß sie die Funktion eines Entropie-Speichers hat. Ein Entropie-Speicher ist beispielsweise eine Schieberegisteranordnung mit linearer Rückkopplung, wie sie beispielsweise als Pseudozufallszahlengenerator zum Einsatz kommt, derart, daß ausgehend von einem bestimmten Ausgangszustand ("Seed") eine mit demselben in nicht-linearem Zusammenhang stehende Ausgangsgröße erzeugt wird, die dazu verwendet wird, um die rückgekoppelte Inverterkette zu stören.

Ein Vorteil der vorliegenden Erfindung besteht darin, daß der erfindungsgemäße Zufallszahlengenerator, da er im wesentlichen aus Digitalschaltungen aufgebaut werden kann, mit bestehenden Prozessen integrierbar ist.

Ein weiterer Vorteil der vorliegenden Erfindung besteht darin, daß der erfindungsgemäße Zufallszahlengenerator mit bestehenden Schaltungsentwurfswerkzeugen synthetisierbar ist und nicht für jede Anwendung als eigenes Full-Custom-Design ausgeführt werden muß.

Ein weiterer Vorteil der vorliegenden Erfindung besteht darin, daß insbesondere bei kryptographischen Anwendungen solche Komprimierungsfunktionen oder Einwegfunktionen oder Entropiespeicher ohnehin vorhanden sind und somit für den Zufallszah-

lengenerator nicht extra implementiert werden müssen, wodurch zusätzliche Chipfläche verbraucht werden würde, sondern von verschiedenen Schaltungsteilen gemeinsam benutzt werden können.

Bevorzugte Ausführungsbeispiele der vorliegenden Erfindung werden nachfolgend Bezug nehmend auf die beiliegenden Zeichnung detailliert erläutert. Es zeigen:

Fig. 1 ein Prinzipblockschaltbild eines erfindungsgemäßen Zufallszahlengenerators;

Fig. 2 einen erfindungsgemäßen Zufallszahlengenerator mit zwei rückgekoppelten Inverterketten und einer nicht-linearen Funktion f;

Fig. 3 einen erfindungsgemäßen Zufallszahlengenerator mit einer von einer Funktion f gesteuerten schaltbaren Kapazität; und

Fig. 4 einen bekannten Zufallszahlengenerator mit zwei rückgekoppelten Inverterketten.

Fig. 1 zeigt einen erfindungsgemäßen Zufallszahlengenerator mit zumindest einer rückgekoppelten Inverterkette 10, einer Ausgabeeinrichtung 12, einer Verarbeitungseinrichtung 14 sowie einer oder mehreren weiteren rückgekoppelten Inverterketten 16, der bzw. denen ebenfalls weitere Verarbeitungseinrichtungen (in Fig. 1 nicht gezeigt) zugeordnet sein können. Die rückgekoppelte Inverterkette 10 besteht beispielsweise aus drei in Kaskade geschalteten rückgekoppelten Invertern, wobei immer ein Ausgang eines Inverters mit einem Eingang des nachfolgenden Inverters verbunden ist. Der Ausgang des Inver-

ters 18a ist ferner über eine Rückkopplungsschleife 20 mit einem Eingang des Inverters 18c verbunden, wie es in Fig. 1 gezeigt ist.

Die Ausgabeeinrichtung 12 dient zum Ausgeben einer Zufallszahl, die von einem Zustand zwischen zwei Invertern der rückgekoppelten Inverterkette abhängt. Bei dem in Fig. 1 gezeigten Ausführungsbeispiel hängt die Zufallszahl von dem Zustand zwischen dem Inverter 18a und dem Inverter 18c ab. Die Ausgabeeinrichtung kann, insbesondere wenn eine zweite Inverterkette 16 vorhanden ist, ebenfalls wie bei bekannten Invertern einen Abtaster und ein nachgeschaltetes XOR-Glied haben, um die Zustände der einzelnen Inverterketten miteinander zu verkoppeln.

Die Verarbeitungseinrichtung 14 ist über Leitungen 22a, 22b mit der rückgekoppelten Inverterkette 10 verkoppelt, um ein Signal zwischen zwei aufeinanderfolgenden Invertern, wie z. B. den Invertern 18a, 18c, wie es in Fig. 1 gezeigt ist, auszukoppeln (Leitung 22a), dann zu verarbeiten, wobei diese Verarbeitung vorzugsweise nicht-linear ist, und dann das verarbeitete Signal, das sich von dem ausgekoppelten Signal unterscheidet, über die Leitung 22b wieder in die rückgekoppelte Inverterkette einzuspeisen. Die Auskopplung und Einspeisung kann an derselben Stelle stattfinden, dahingehend, daß zwischen den beiden aufeinanderfolgenden Invertern, aus denen das Signal über die Leitung 22b ausgekoppelt worden ist, auch das verarbeitete Signal wieder eingespeist wird. Dieser Fall ist beispielsweise in Fig. 1 gezeigt. Alternativ kann jedoch auch die Ein-Auskopplung zwischen unterschiedlichen Inverterpaaren erfolgen. So könnte die Einkopplung beispielsweise auch zwischen den Invertern 18c, 18b oder zwischen den Invertern 18b, 18a erfolgen.

Wie es durch eine gestrichelte Verbindungsleitung 24 dargestellt ist, kann die Aus- und Einkopplung über die Leitung 22a und 22b derart erfolgen, daß die Verarbeitungseinrichtung Teil der Rückkopplung der rückgekoppelten Inverterkette wird. In diesem Fall wäre die gestrichelte Verbindungsleitung 24 nicht vorhanden. Alternativ kann das von der Verarbeitungseinrichtung gelieferte Signal, das über die Leitung 22b der rückgekoppelten Inverterkette zugeführt wird, auch mit dem auf der Verbindungsleitung 24 vorhandenen Signal kombiniert werden, derart, daß die Verbindungsleitung 24 vorhanden ist und am Berührungspunkt zwischen der Leitung 22b und der Leitung 24 ein Kombinierer z. B. in Form eines Addierers, Subtrahierers, logischen Gatters etc. vorhanden ist. Wie es Bezug nehmend auf Fig. 3 ausgeführt ist, kann die Einspeiseleitung 22b auch periodisch an- und abgetrennt werden, derart, daß die rückgekoppelte Inverterkette 10 dahingehend asynchron beeinflußt wird, daß zu bestimmten Zeitpunkten die Verarbeitungseinrichtung angekoppelt ist und zu bestimmten alternativen Zeitpunkten nicht angekoppelt ist.

Wie es bereits ausgeführt worden ist, kann der erfindungsgemäße Zufallszahlengenerator auch über eine weitere Inverterkette 16 verfügen, die vorzugsweise eine andere Anzahl von Invertern aufweist als die erste Inverterkette 10. Der weiteren rückgekoppelten Inverterkette 16 kann ferner eine Verarbeitungseinrichtung zugeordnet sein oder nicht. Lediglich wesentlich für die Qualität der Zufallszahlen, die der erfindungsgemäße Zufallszahlengenerator liefert, ist, daß die beiden Inverterketten 16 nicht einen irgendwie auch immer gearteten synchronen Zustand einnehmen. Dies wird dadurch verhindert, daß in einer Inverterkette, nämlich der Inverterkette 10 die Verarbeitungseinrichtung 14 aktiv ist, während in der

anderen Inverterkette 16 keine Verarbeitungseinrichtung aktiv ist oder eine weitere Verarbeitungseinrichtung aktiv, die sich von der ersten Verarbeitungseinrichtung 14 unterscheidet.

Im nachfolgenden wird Bezug nehmend auf Fig. 2 ein bevorzugtes Ausführungsbeispiel der vorliegenden Erfindung dargestellt. Der erfindungsgemäße Zufallszahlengenerator umfaßt eine erste rückgekoppelte Inverterkette 10 mit drei in Kaskade geschalteten Invertern 18a, 18b, 18c und der Rückkopplungsleitung 20. Der Inverter umfaßt ferner eine zweite rückgekoppelte Inverterkette 16 mit den Invertern 24a bis 24e. Der rückgekoppelten Inverterkette 10 sind nunmehr, wie es in Fig. 2 gezeigt ist, eine zweiteilige Verarbeitungseinrichtung zugeordnet, die eine erste Teilverarbeitungseinrichtung 14a umfaßt, die den Kondensator C_3, der zwischen den Invertern 18a und 18c einerseits und einer Schaltungsmasse andererseits geschaltet ist. Eine weitere Teil-Verarbeitungseinrichtung ist durch eine Funktion f gezeigt und mit 14b bezeichnet. Die Funktion f verarbeitet ein Signal zwischen den beiden Invertern 18a, 18c und speist ein verarbeitetes Signal zwischen die beiden Inverter 18a, 18c ein. Die Funktion f als Verarbeitungseinrichtung könnte jedoch auch das verarbeitete Signal, also das Ausgangssignal der Funktion an anderer Stelle einspeisen, wie z. B. zwischen die rückgekoppelten Inverter 18c, 18b oder die rückgekoppelten Inverter 18b, 18a.

Der weiteren Inverterkette 16 ist ferner bei dem in Fig. 2 gezeigten bevorzugten Ausführungsbeispiel eine Verarbeitungseinrichtung in Form eines Kondensators C_1, der mit 26 bezeichnet ist, zugeordnet, die zwischen den beiden Invertern 24e, 24d wirksam ist. Ferner ist der weiteren Inverterkette 16 noch eine zusätzliche Verarbeitungseinrichtung 28 in Form

des Kondensators C_2 zwischen den beiden Invertern 24a, 24b und der Masse der Schaltung zugeordnet.

Die Kondensatoren C_1, C_2, C_3, die die Verarbeitungseinrichtungen 26, 28, 14a darstellen, bewirken eine nicht-lineare Phasenverschiebung hinsichtlich der Frequenz und stellen somit eine nicht-lineare Verzögerung dar, die einen weiteren Vorteil hat. Die Verwendung von parallel geschalteten Kondensatoren genauso wie von seriell geschalteten Spulen oder LC-Gliedern oder RC-Gliedern führt zu einer Verringerung der Schwingfrequenz der Inverterketten. Damit wird die Anzahl der Umschaltvorgänge der typischerweise in CMOS-Technik ausgeführten Invertern pro Zeiteinheit reduziert, was in einem geringeren Stromverbrauch der Inverterketten resultiert. Der geringere Stromverbrauch ist besonders für Kontaktlosanwendungen von Interesse, jedoch auch für z. B. batteriebetriebene Anwendungen von Vorteil, da die Batterielebensdauer vergrößert wird.

Die Funktion 14b kann, wie es ausgeführt worden ist, eine kryptographisch starke Komprimierungsfunktion, wie z. B. eine Hash-Funktion sein. Die Funktion f kann ferner eine Einwegfunktion sein, die sich ebenfalls durch eine starke Nichtlinearität auszeichnet, oder aber ein Entropiespeicher in Form einer rückgekoppelten Schieberegisterkette. Allgemein ist die kryptographische Funktion f so ausgestaltet, daß sie eine möglichst große "Unruhe" in der rückgekoppelten Inverterkette, auf die sie einwirkt, stiftet.

Im Gegensatz zu dem in Fig. 2 gezeigten Ausführungsbeispiel kann die Funktion f auch dazu verwendet werden, einen Schalter 30 anzusteuern, derart, daß je nach Ausgangssignal der Funktion f, also abhängig davon, ob die Funktion f einen "0"-

Zustand oder einen "1"-Zustand ausgibt, die Verarbeitungseinrichtung 14a der rückgekoppelten Inverterkette 10 zugeschaltet oder von derselben abgekoppelt wird. Auch durch diese Vorgehensweise wird die rückgekoppelte Inverterkette aperiodisch beeinflußt, so daß das Problem des identischen Samplens mittels der Ausgabeeinrichtung in Form des Abtasters 12a und das Gatters 12b minimiert wird.

Schließlich sei darauf hingewiesen, daß je nach Anwendungsfall und Anforderung jeder Inverterkette eine oder mehrere Verarbeitungseinrichtungen zugeordnet werden kann bzw. können, und daß, wenn mehrere parallele Inverterketten eingesetzt werden, die parallelen Inverterketten durch Verarbeitungseinrichtungen unterschiedlich beeinflußt werden, um eine möglichst zufällige Zufallszahl am Ausgang der Ausgabeeinrichtung 12 (Fig. 1) zu erzeugen.

Bezugszeichenliste

10 rückgekoppelte Inverterkette
12a Abtaster
12 Ausgabeeinrichtung
12b XOR-Gatter
14 Verarbeitungseinrichtung
14a erste Teilverarbeitungseinrichtung
14b zweite Teilverarbeitungseinrichtung
16 weitere rückgekoppelte Inverterkette
18a Inverter
18b Inverter
18c Inverter
20 Rückkopplungsschleife
22a Auskopplungsleitung
22b Einkopplungsleitung
24 Überbrückungsleitung
24a Inverter
24b Inverter
24c Inverter
24d Inverter
24e Inverter
26 weitere Verarbeitungseinrichtung
28 noch weitere Verarbeitungseinrichtung
30 Schalter
40 rückgekoppelte Inverterkette
41 Rückkopplungsleitung
40a Inverter
40b Inverter
40c Inverter
42 weitere rückgekoppelte Inverterkette
42a Inverter
42b Inverter

42c Inverter
43 weitere Rückkopplungsleitung
44 Abtaster
45 XOR-Gatter
46a erste Abtastausgangsleitung
46b zweite Abtastausgangsleitung

Patentansprüche

1. Zufallszahlengenerator mit folgenden Merkmalen:

einer rückgekoppelten Inverterkette (10) mit kaskadierten Invertern (18a, 18b, 18c);

einer Ausgabeeinrichtung (12) zum Ausgeben einer Zufallszahl, die von einem Zustand zwischen zwei Invertern (18a, 18c) der rückgekoppelten Inverterkette (10) abhängt; und

einer Verarbeitungseinrichtung (14) zum Verarbeiten eines Signals zwischen zwei aufeinanderfolgenden Invertern (18a, 18c) der kaskadierten Inverter und zum Einspeisen (22b) eines verarbeiteten Signals in die rückgekoppelte Inverterkette, wobei die Verarbeitungseinrichtung (14) so ausgebildet ist, daß sich das verarbeitete Signal von dem unverarbeiteten Signal unterscheidet.

2. Zufallszahlengenerator nach Anspruch 1,

bei dem die Verarbeitungseinrichtung (14) ausgebildet ist, um eine nicht-lineare Verarbeitung auszuführen.

3. Zufallszahlengenerator nach Anspruch 1 oder 2,

bei dem die Verarbeitungseinrichtung (14) ein Verzögerungsglied (14a, 26, 28) umfaßt.

4. Zufallszahlengenerator nach Anspruch 3,

bei dem das Verzögerungsglied eine Kapazität (C1, C2, C3) umfaßt, die zwischen einer Verbindungsleitung (20) zwischen den

aufeinanderfolgenden Invertern und ein Bezugspotential geschaltet ist, oder eine serielle Induktivität oder sowohl die Kapazität als auch die Induktivität aufweist.

5. Zufallszahlengenerator nach einem der vorhergehenden Ansprüche,

bei dem die Verarbeitungseinrichtung (14) ausgebildet ist, um ein Ausgangssignal des einen der zwei aufeinanderfolgenden Inverter zu verarbeiten und ein verarbeitetes Signal in einen Eingang des anderen der aufeinanderfolgenden Inverter einzuspeisen.

6. Zufallszahlengenerator nach einem der vorhergehenden Ansprüche,

bei dem die Verarbeitungseinrichtung (14) ausgebildet ist, um eine Komprimierungsfunktion, insbesondere eine Hash-Funktion oder eine Einwegfunktion auszuführen.

7. Zufallszahlengenerator nach einem der vorhergehenden Ansprüche,

bei dem die Verarbeitungseinrichtung (14) ausgebildet ist, um einen Entropiespeicher zu umfassen.

8. Zufallszahlengenerator nach Anspruch 7,

bei dem der Entropiespeicher ein rückgekoppeltes Schieberegister aufweist.

9. Zufallszahlengenerator nach einem der vorhergehenden Ansprüche,

der ferner eine steuerbare Schalteinrichtung (30) aufweist, um das verarbeitete Signal abhängig von dem Steuersignal in die rückgekoppelte Inverterkette (10) einzuspeisen oder nicht einzuspeisen.

10. Zufallszahlengenerator nach Anspruch 9,

bei dem das steuerbare Signal gleich einem Signal aus der Inverterkette ist oder von dem Signal mittels einer Funktion (14b) abgeleitet ist.

11. Zufallszahlengenerator nach Anspruch 10,

bei dem die Funktion eine Komprimierungsfunktion oder eine Einwegfunktion oder eine durch ein rückgekoppeltes Schieberegister implementierte Funktion ist.

12. Zufallszahlengeneratoren nach einem der vorhergehenden Ansprüche, der ferner folgende Merkmale aufweist:

eine weitere rückgekoppelte Inverterkette (16);

eine Abtasteinrichtung (12a) zum Abtasten eines Signals der rückgekoppelten Inverterkette und eines Signals der weiteren rückgekoppelten Inverterkette;

eine Verknüpfungseinrichtung (12b) zum Verknüpfen der abgetasteten Signale, um eine Zufallszahl zu erzeugen.

13. Zufallszahlengenerator nach Anspruch 12,

bei dem die weitere Inverterkette keine Verarbeitungseinrichtung aufweist.

14. Zufallszahlengenerator nach Anspruch 12,

bei dem der weiteren Inverterkette (16) eine weitere Verarbeitungseinrichtung (26, 28) zugeordnet ist, die sich von der Verarbeitungseinrichtung (14), die der Inverterkette (10) zugeordnet ist, hinsichtlich ihrer Verarbeitung unterscheidet.

15. Zufallszahlengenerator nach Anspruch 14,

bei dem der weiteren Inverterkette (16) neben der weiteren Verarbeitungseinrichtung (26) noch eine zusätzliche Verarbeitungseinrichtung (28) zugeordnet ist, die ein verarbeitetes Signal zwischen zwei anderen aufeinanderfolgenden Invertern (24a, 24b) einspeist als dies die andere Verarbeitungseinrichtung (26) durchführt, die der weiteren Inverterkette (16) zugeordnet ist.

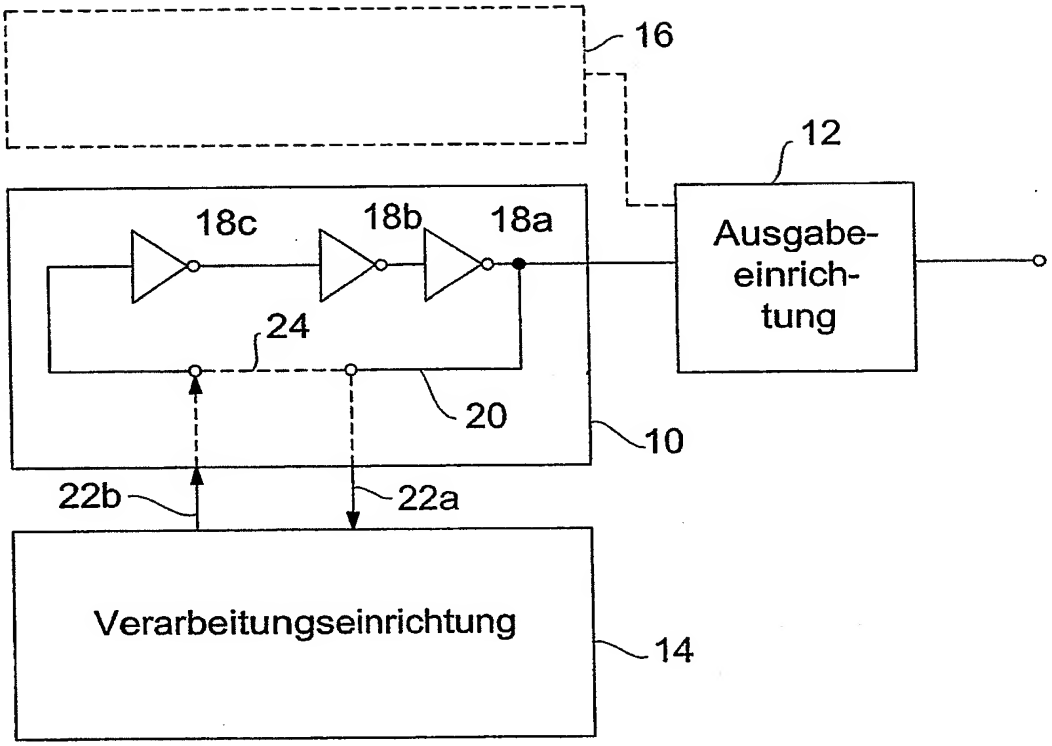


FIG 1

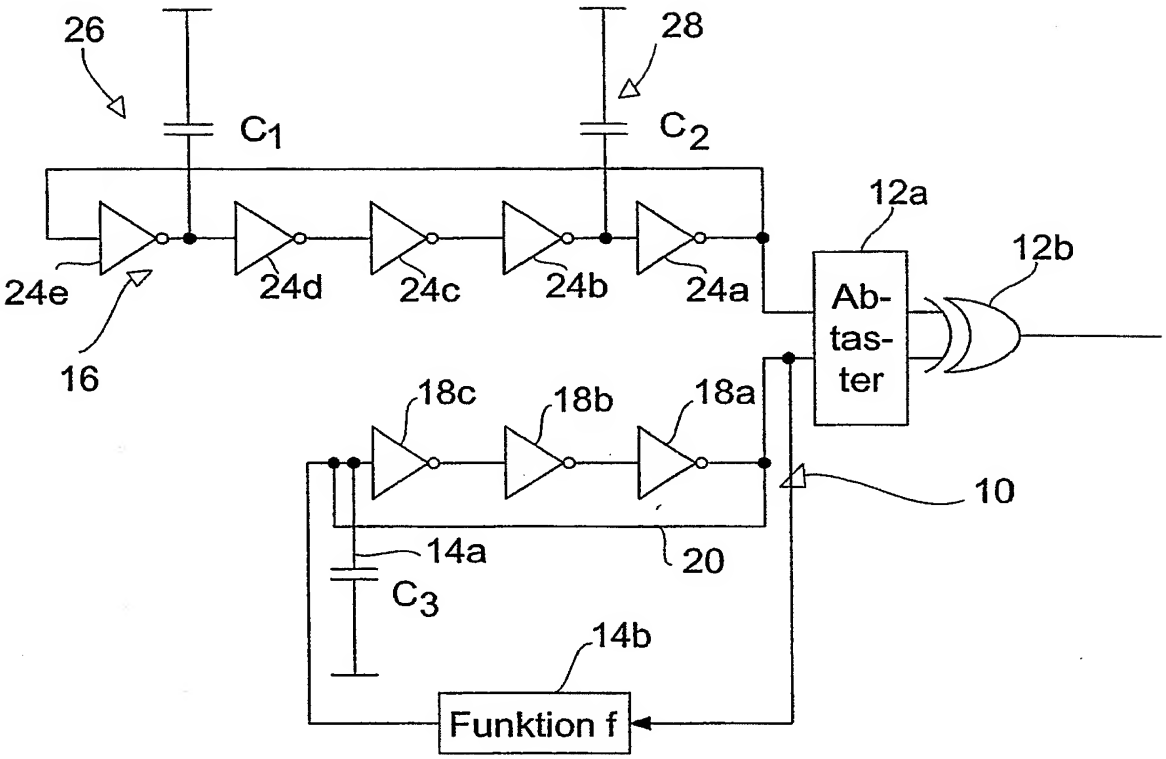


FIG 2

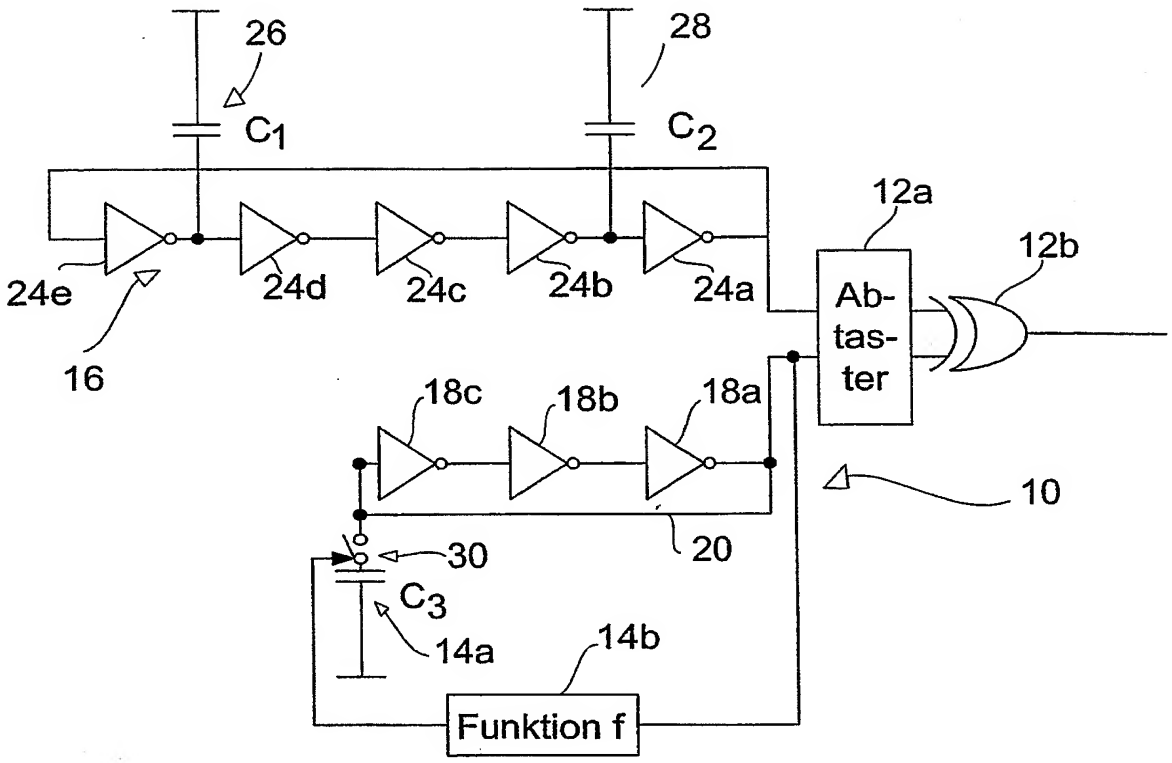


FIG 3

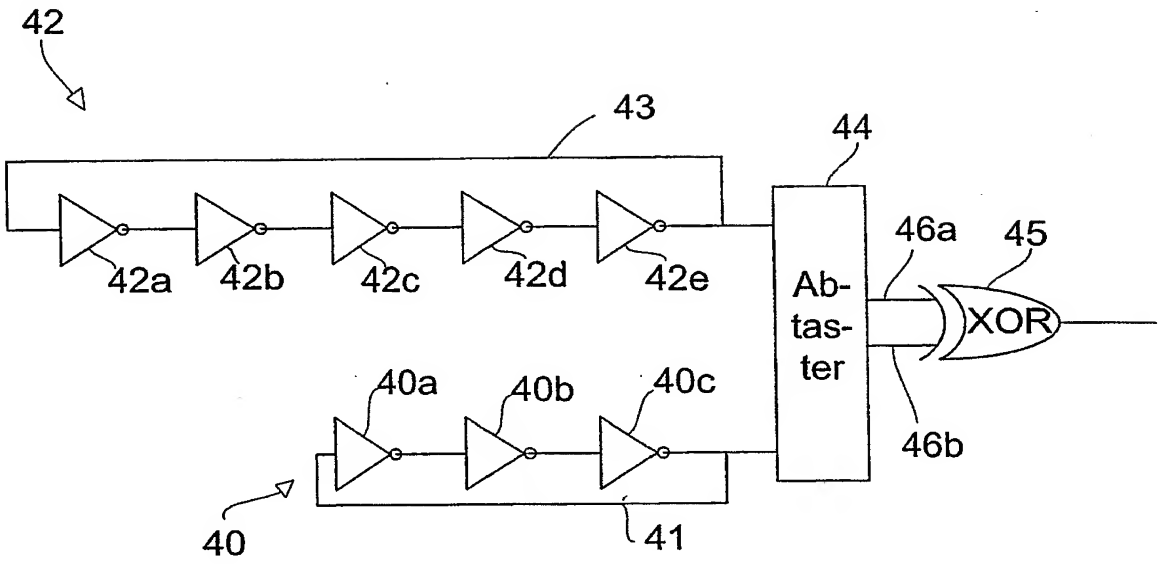


FIG 4